**UNITED STATES DISTRICT COURT**
**DISTRICT OF MINNESOTA**

| | |
|---|---|
| Klowie Fields and Ryan O'Connell, individually, and on behalf of all others similarly situated,<br><br>Plaintiffs,<br><br>v.<br><br>Arrowhead Regional Computing Consortium,<br><br>Defendant. | Case No.:<br><br><br><br>**CLASS ACTION COMPLAINT**<br><br>JURY TRIAL DEMANDED |

Plaintiffs Klowie Fields and Ryan O'Connell (collectively, "Plaintiffs"), individually, and on behalf of all others similarly situated, bring this action against Arrowhead Regional Computing Consortium ("ARCC" or "Defendant"). Plaintiffs bring this action by and through their attorneys, and allege, based upon personal knowledge as to their own actions, and based upon information, belief, and reasonable investigation by their counsel as to all other matters, as follows.

## I. INTRODUCTION

1. ARCC is a company that provides payroll and finance services along with student information systems to over fifty school districts in northeast Minnesota.[1]

2. As part of its services, ARCC collects, maintains, and stores highly sensitive personal and private information belonging to its employees, and current and former students and staff in the school districts that ARCC serves, including, but not limited to:

[1] https://www.arcc.org/ (last accessed January 22, 2024).

Social Security numbers, full names, student educational records (collectively, "personally identifying information" or "PII"), health insurance information, and medical information including medical conditions and treatment (collectively, "protected health information" or "PHI"; with PII, "Private Information").

3. On February 6, 2023, ARCC experienced a data breach incident (the "Data Breach") in which an unauthorized party accessed its network environment. Subsequently, ARCC determined that the unauthorized party was able to remove some of the sensitive data from its network.

4. On December 7, 2023, ARCC discovered that the Data Breach impacted Private Information belonging to more than 65,000 individuals that provided their Private Information to ARCC. On January 11, 2024, ARCC issued data breach notices to individuals whose information was believed to have been accessed in this incident, including Plaintiffs and Class members.

5. As ARCC stored and handled such highly-sensitive Private Information, it had a duty and obligation to safeguard this information and prevent unauthorized third parties from accessing this data.

6. Ultimately, ARCC failed to fulfill these obligations as an unauthorized party breached ARCC's information systems and databases and accessed vast quantities of Private Information belonging to Plaintiffs and Class members. This breach and the successful exfiltration of Private Information were direct, proximate, and foreseeable results of multiple failings on the part of ARCC.

7. The data breach occurred because ARCC inexcusably failed to implement reasonable security protections to safeguard its information systems and databases. Prior to the Data Breach, ARCC failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiffs and Class members been made aware of this fact, they would have never provided their Private Information to ARCC.

8. ARCC's meager attempt to ameliorate the effects of the Data Breach with *one year* of complimentary credit monitoring is woefully inadequate. Much of the Private Information that was stolen is immutable and one year of credit monitoring is nothing in the face of a life-long heightened risk of identity theft.

9. As a result of ARCC's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its statutory, and common-law obligations, Plaintiffs and Class members suffered injuries as a result of ARCC's conduct including, but not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;
- Time needed to change usernames and passwords on their accounts;
- Time needed to investigate, correct and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach;

- Charges and fees associated with fraudulent charges on their accounts; and the continued and increased risk of compromise to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their Private Information.

10. Accordingly, Plaintiffs bring this action on behalf of all those similarly situated to seek relief for the consequences of Defendant's failure to reasonably safeguard Plaintiffs' and Class members' Private Information; its failure to reasonably provide timely notification that Plaintiffs' and Class members' Private Information had been compromised by an unauthorized third party; and for intentionally and unconscionably deceiving Plaintiffs and Class members concerning the status, safety, location, access, and protection of their Private Information.

## II. PARTIES

**Plaintiff Klowie Fields**

11. Plaintiff Fields is a resident of Chisholm, Minnesota, and was a student in Independent School District 318 from 1987 to 2000. Plaintiff Fields also served as a teacher in Independent School District 318 from 2001 to 2002.

**Plaintiff Ryan O'Connell**

12. Plaintiff O'Connell is a resident of Virginia, Minnesota, and was a student in Independent School District 706 from 1987 to 2000.

**Defendant ARCC**

13. Defendant ARCC is a Minnesota company with its principal place of business at 4884 Miller Trunk Hwy, Suite 300, Hermantown, Minnesota 55811.

## III. JURISDICTION AND VENUE

14. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, the number of class members exceeds 100, and at least one Class member is a citizen of a state different from Defendant.

15. This Court has personal jurisdiction over Defendant because Defendant is a resident of Minnesota, conducts business in this District, and the acts and omissions giving rise to the claims alleged herein occurred in and emanated from this District.

16. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because ARCC resides in this District and is being served in this District.

## IV. FACTUAL ALLEGATIONS

### A. ARCC – Background

17. ARCC is a payroll and finance services company whose mission is "to provide services, deliver training, and promote innovation to support [Minnesota] regions school districts."[2] ARCC assists with all aspects of district payroll, trains and supports in the areas of SMART systems and Minnesota school finance and accounting, provides support for state reporting, student information systems, and some third-party integrations. As part of its operations, Defendant collects, maintains, and stores the highly sensitive Private Information provided by its current and former employees, and current and former

[2] https://www.arcc.org/ (last accessed January 22, 2024).

students and staff, including but not limited to: Social Security numbers, full names, student educational records, health insurance information, and medical information including medical conditions and treatment.

18. On information and belief, ARCC had failed to implement necessary data security safeguards at the time of the Data Breach. This failure resulted in a third party's unauthorized access of the Private Information of ARCC's current and former employees, students, and educators—Plaintiffs and Class members.

19. Individuals such as the Plaintiffs, made their Private Information available to ARCC with the reasonable expectation that any entity with access to this information would keep that sensitive and personal information confidential and secure from illegal and unauthorized access. And, in the event of any unauthorized access, that ARCC would provide them with prompt and accurate notice.

20. This expectation was objectively reasonable and based on an obligation imposed on ARCC by statute, regulations, industrial custom, and standards of general due care.

21. Unfortunately for Plaintiffs and Class members, ARCC failed to carry out its duty to safeguard sensitive Private Information and provide adequate data security. As a result, it failed to protect Plaintiffs and Class members from having their Private Information accessed during the Data Breach.

## B. The Data Breach

22. According to the Notice of Data Breach provided by Defendant, on or about February 6, 2023, ARCC discovered unauthorized access to its computer network environment.

23. On December 7, 2023—*ten months* after ARCC discovered the Data Breach—ARCC confirmed that Plaintiffs' and Class members' Private Information was accessed by an unauthorized party.

24. On January 11, 2024, nearly *one year* after ARCC first discovered the breach, ARCC sent notices to all individuals affected by the Data Breach.

## C. ARCC's Many Failures Both Prior to and Following the Breach

25. Defendant collects and maintains vast quantities of Private Information belonging to Plaintiffs and Class members as part of its normal operations. The data breach occurred as direct, proximate, and foreseeable results of multiple failings on the part of Defendant.

26. First, Defendant failed to implement reasonable security protections to safeguard its information systems and databases.

27. Second, Defendant failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiffs and Class members been aware that Defendant did not have adequate safeguards in place to protect such sensitive Private Information, they would have never provided such information to Defendant.

28. Third, Defendant did not inform Plaintiffs and Class members that their information was stolen until nearly one year after it first discovered the Data Breach. This

delay in informing victims virtually ensured that the unauthorized parties who accessed this Private Information could monetize, misuse and/or disseminate that Private Information before Plaintiffs and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiffs and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

29. Fourth, Defendant's attempt to ameliorate the effects of this Data Breach with one year of complimentary credit monitoring is inadequate. Plaintiffs' and Class members' Private Information was accessed and acquired by an unauthorized party. As a consequence, they face the real, immediate, and likely danger of identity theft and misuse of their Private Information. And this can, and in some circumstances already has, caused irreparable harm to their personal, financial, reputational, and future well-being. This harm is even more acute because much of the accessed Private Information is immutable.

30. In short, Defendant's myriad failures, including the failure to timely notify Plaintiffs and Class members that their personal and financial information had been accessed without permission due to Defendant's security failures, allowed unauthorized individuals to access, misappropriate, and misuse Plaintiffs' and Class members' Private Information for more than two months before Defendant finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

**D. Data Breaches Pose Significant Threats**

31. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors. It is well known that PII, Social Security numbers in particular, are an invaluable commodity and a frequent target of hackers.

32. In 2022, the Identity Theft Resource Center's Annual End-of-Year Data Breach Report listed 1,802 total compromises involving 422,143,312 victims for 2022, which was just 50 compromises short of the current record set in 2021.[3] The HIPAA Journal's 2022 Healthcare Data Breach Report reported 707 compromises involving healthcare data, which is just eight shy of the record of 715 set in 2021 and still double that of the number of similar such compromises in 2017 and triple the number of compromises in 2012.[4]

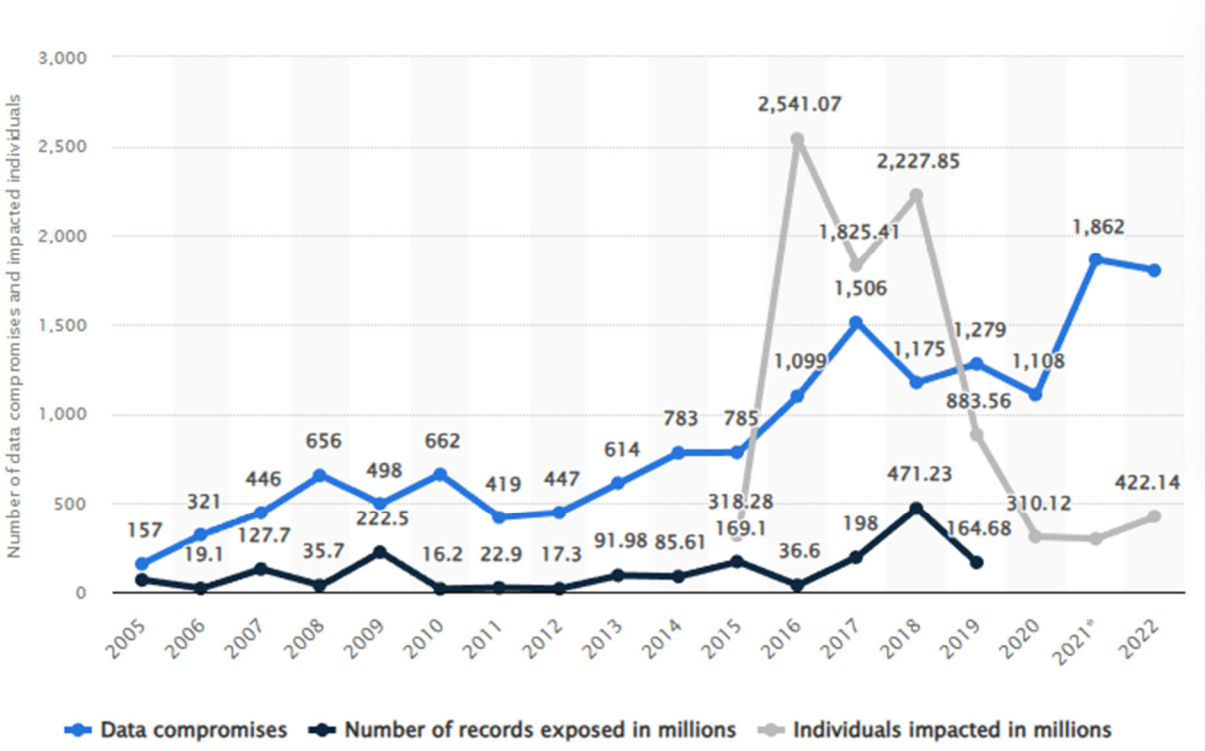
33. Statista, a German entity that collects and markets data relating to, among other things, data breach incidents and the consequences thereof, confirms that the number of data breaches has been steadily increasing since it began a survey of data compromises in 2005 with 157 compromises reported that year, to a peak of 1,862 in 2021, to 2022's total of 1,802.[5] The number of impacted individuals has also risen precipitously from

[3] *2022 End of Year Data Breach Report*, Identity Theft Resource Center (January 25, 2023), available at: https://www.idtheftcenter.org/publication/2022-data-breach-report/?utm_source=press+release&utm_medium=web&utm_campaign=2022+Data+Breach+Report+.

[4] *2022 Healthcare Data Breach Report*, The HIPAA Journal (January 24, 2023), available at: https://www.hipaajournal.com/2022-healthcare-data-breach-report/.

[5] *Annual Number of Data Breaches and Exposed Records in the United States from 2005*

approximately 318 million in 2015 to 422 million in 2022, which is an increase of nearly 50%.[6]




34. This stolen PII is then routinely traded on dark web black markets as s simple commodity, with Social Security numbers being so ubiquitous to be sold at as little as $2.99 apiece and passports retailing for as little as $15 apiece.[7]

35. In addition, the severity of the consequences of a compromised social security number belies the ubiquity of stolen numbers on the dark web. Criminals and other

*to 2022*, Statista, available at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

[6] *Id.*

[7] *What is your identity worth on the dark web?* Cybernews (September 28, 2021), available at: https://cybernews.com/security/whats-your-identity-worth-on-dark-web/.

unsavory elements can fraudulently take out loans under the victims' name, open new lines of credit, and cause other serious financial difficulties for victims:

> [a] dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[8]

36. This is exacerbated by the fact that the problems arising from a compromised social security number are exceedingly difficult to resolve. A victim is forbidden from proactively changing his or her number unless and until it is actually misused and harm has already occurred. And even this delayed remedial action is unlikely to undo the damage already done to the victims:

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.[9]

37. In addition, the Federal Trade Commission ("FTC") has brought dozens of cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data, including recent cases concerning

[8] United States Social Security Administration, *Identity Theft and Your Social Security Number*, United States Social Security Administration (July 2021), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.
[9] *Id.*

health-related information against LabMD, Inc., SkyMed International, Inc., and others. The FTC publicized these enforcement actions to place companies like Defendant on notice of its obligation to safeguard former and current employee information.[10]

38. Given the nature of Defendant's Data Breach, as well as the long delay in notification to the Class, it is foreseeable that the compromised Private Information has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the unauthorized parties who possess Plaintiffs' and Class members' Private Information can easily obtain Plaintiffs' and Class members' tax returns or open fraudulent credit card accounts in Class members' names.

39. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[11] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

40. To date, Defendant has offered its consumers only one year of identity theft monitoring services. The offered services are inadequate to protect Plaintiffs and the Class

[10] *See e.g.*, *In the Matter of SKYMED INTERNATIONAL, INC.*, C-4732, 1923140 (F.T.C. Jan. 26, 2021).

[11] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes (Mar 25, 2020), available at https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1. *See also Why Your Social Security Number Isn't as Valuable as Your Login Credentials*, Identity Theft Resource Center (June 18, 2021), available at https://www.idtheftcenter.org/post/why-your-social-security-number-isnt-as-valuable-as-your-login-credentials/.

from the threats they will face for years to come, particularly in light of the Private Information at issue here.

41. Despite the prevalence of public announcements of data breach and data security compromises, its own acknowledgment of the risks posed by data breaches, and its own acknowledgment of its duties to keep Private Information private and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and the Class from misappropriation. As a result, the injuries to Plaintiffs and the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures.

## E. ARCC Had a Duty and Obligation to Protect Private Information

42. Defendant has an obligation to protect the Private Information belonging to Plaintiffs and Class members. First, this obligation was mandated by government regulations and state laws, including FTC rules and regulations. Second, this obligation arose from industry standards regarding the handling of sensitive PII and employment records. And, third, Defendant imposed such an obligation on itself with its promises regarding the safe handling of data.[12] Plaintiffs and Class members provided, and Defendant obtained, their information on the understanding that it would be protected and safeguarded from unauthorized access or disclosure.

[12] *See ARCC Privacy Notice*, (last upd. August 5, 2021), available at https://www.ARCC.com/wp-content/uploads/sites/2/2021/08/ARCC-Privacy-Notice_21-08-05.pdf

### 1. FTC Act Requirements and Violations

43. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

44. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[13] The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.[14] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[15]

---

[13] *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n (October 2016), available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.
[14] *Id.*
[15] *Id.*

45. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

46. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

47. Additionally, the FTC Health Breach Notification Rule obligates companies that suffered a data breach to provide notice to every individual affected by the data breach, as well as notifying the media and the FTC. *See* 16 CFR 318.1, *et seq.*

48. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

49. Defendant was fully aware of its obligation to protect the Private Information of its current and former employees and former Minnesota school district alumni, including Plaintiffs and the Class, and on information and belief, Defendant is a sophisticated and technologically savvy entity that relies extensively on technology systems and networks to

maintain its practice, including storing its employees' PII, private information, and other uniquely identifying information in order to operate its business.

50. Defendant had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting the Private Information from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between Defendant and Plaintiffs and Class members. Defendant alone had the exclusive ability to implement adequate security measures to its cyber security network to secure and protect Plaintiffs' and Class members' Private Information.

**2. Industry Standards and Noncompliance**

51. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

52. Some industry best practices that should be implemented by businesses dealing with sensitive Private Information like Defendant include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

53. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems;

and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

54. Defendant should have also followed the minimum standards of any one of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

55. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

56. Further, Defendant delayed almost one year between discovering the breach and issuing notice. This delay was beyond what is reasonable acceptable or statutorily mandated.

## F. Plaintiffs and the Class Suffered Harm Resulting from the Data Breach

57. Like any data hack, the Data Breach presents major problems for all affected.[16]

58. The FTC warns the public to pay particular attention to how they keep personally identifying information including Social Security numbers and other sensitive data. As the FTC notes, "once identity thieves have your personal information, they can

[16] Paige Schaffer, *Data Breaches' Impact on Consumers*, Insurance Thought Leadership (July 29, 2021), available at https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers.

drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[17]

59. The ramifications of Defendant's failure to properly secure Plaintiffs' and Class members' Private Information are severe. Identity theft occurs when someone uses another person's financial, and personal information, such as that person's name, address, Social Security number, and other information, without permission in order to commit fraud or other crimes.

60. According to data security experts, one out of every four data breach notification recipients become a victim of identity fraud.

61. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

62. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. According to a recent study published in the scholarly journal *Preventive Medicine Reports*, public and corporate data breaches correlate to an increased risk of identity theft for victimized consumers.[18] The same study also found that identity theft is a deeply traumatic event for the victims, with

[17] *Warning Signs of Identity Theft*, Federal Trade Comm'n, available at https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft.

[18] David Burnes, Marguerite DeLiema, Lynn Langton, *Risk and protective factors of identity theft victimization in the United States*, Preventive Medicine Reports, Volume 17 (January 23, 2020), available at https://www.sciencedirect.com/science/article/pii/S2211335520300188?via%3Dihub.

more than a quarter of victims still experiencing sleep problems, anxiety, and irritation even six months after the crime.[19]

63. There is also a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals presents a concrete risk that the cybercriminals who now possess Class members' Private Information will do so at a later date or re-sell it.

64. Data breaches have also proven to be costly for affected organizations as well, with the average cost to resolve being $4.45 million dollars in 2023.[20] The average cost to resolve a data breach involving health information, however, is more than double this figure at $10.92 million.[21]

65. In response to the Data Breach, Defendant offered to provide certain individuals whose Private Information was exposed in the Data Breach with just one year of credit monitoring through IDX. However, this is much shorter than what is necessary to protect against the lifelong risk of harm imposed on Plaintiffs and Class members by Defendant's failures.

---

[19] *Id.*
[20] *Cost of a Data Breach Report 2023*, IBM Security, available at https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX0vRlNbx6p9BpWaOo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD_BwE&gclsrc=aw.ds.
[21] *Id.*

66. Moreover, the credit monitoring offered by Defendant is fundamentally inadequate to protect them from the injuries resulting from the unauthorized access and exfiltration of their sensitive Private Information.

67. Here, due to the Breach, Plaintiffs and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the Private Information stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, if they were fortunate enough to learn of the Data Breach despite Defendant's delay in disseminating notice in accordance with state law;

e. The imminent and impending injury resulting from potential fraud and identity theft posed because their Private Information is exposed for theft and sale on the dark web; and

f. The loss of Plaintiffs' and Class members' privacy.

68. Plaintiffs and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting

from their Private Information being accessed by cybercriminals, risks that will not abate within a couple of years: the unauthorized access of Plaintiffs' and Class members' Private Information, especially their Social Security numbers, puts Plaintiffs and the Class at risk of identity theft indefinitely, and well beyond the limited period of credit monitoring that Defendant offered victims of the Breach.

69. As a direct and proximate result of Defendant's acts and omissions in failing to protect and secure Private Information, Plaintiffs and Class members have been placed at a substantial risk of harm in the form of identity theft, and have incurred and will incur actual damages in an attempt to prevent identity theft.

70. Plaintiffs retains an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both themselves and similarly situated individuals whose Private Information was accessed in the Data Breach.

## G. EXPERIENCES SPECIFIC TO PLAINTIFFS

### Plaintiff Klowie Fields

71. Plaintiff Klowie Fields was a student at the Independent School District 318 from 1987 to 2000, and was a substitute teacher in Independent School District 318 from 2001 to 2002.

72. Plaintiff Fields provided her Private Information to Defendant, through both being a student and a teacher in a school district that engaged ARCC's services.

73. Plaintiff Fields became aware of the Data Breach through the notice Defendant mailed to her. She learned that information such as full names, Social Security

numbers, student educational information, and medical information and treatment information were compromised in the Data Breach.

74. After the Data Breach, Plaintiff Fields experienced a dramatic increase in the number of spam phone calls and marketing emails.

75. As a result of the Data Breach and the resulting suspicious activity, Plaintiff Fields has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. She has also spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including, but not limited to, work and recreation.

76. As a result of the Data Breach, Plaintiff Fields has suffered anxiety due to the public dissemination of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using her private information for purposes of identity theft and fraud. Plaintiff Fields is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

77. Plaintiff Fields suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from her; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

78. As a result of the Data Breach, Plaintiff Fields anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. And, as a result of the Data Breach, she is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

**Plaintiff Ryan O'Connell**

79. Plaintiff Ryan O'Connell was a student in Independent School District 706 from 1987 to 2000.

80. Plaintiff O'Connell provided his Private Information to Defendant through being a student in a school district that engaged ARCC's services.

81. Plaintiff O'Connell became aware of the Data Breach through the notice Defendant mailed to him. He learned that information such as full names, Social Security numbers, student educational information, and medical information and treatment information were compromised in the Data Breach.

82. After the Data Breach, Plaintiff O'Connell experienced a dramatic increase in the number of spam phone calls and marketing emails.

83. As a result of the Data Breach and the resulting suspicious activity, Plaintiff O'Connell has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. He has also spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including, but not limited to, work and recreation.

84. As a result of the Data Breach, Plaintiff O'Connell has suffered anxiety due to the public dissemination of his personal information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using his private information for purposes of identity theft and fraud. Plaintiff O'Connell is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

85. Plaintiff O'Connell suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from him; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

86. As a result of the Data Breach, Plaintiff O'Connell anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. And, as a result of the Data Breach, he is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

## V. CLASS REPRESENTATION ALLEGATIONS

87. Plaintiffs bring this action on behalf of themselves and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Class of:

> All persons in the United States whose Private Information was accessed in the Data Breach.

Excluded from the Class are Defendant, its executives and officers, and the Judge(s) assigned to this case. Plaintiffs reserve the right to modify, change or expand the Class definition after conducting discovery.

88. In the alternative, Plaintiffs brings this action on behalf of themselves and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3),, a subclass of:

> All persons who are residents of the State of Minnesota whose Private Information was accessed in the Data Breach (the "Minnesota Subclass").

Excluded from the Subclass are Defendant, its executives and officers, and the Judge(s) assigned to this case.

89. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. The exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendant and obtainable by Plaintiffs only through the discovery process, upon information and belief tens of thousands of individuals comprise the Class.[22] The members of the Class will be identifiable through information and records in Defendant's possession, custody, and control.

90. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions

[22] According to the Office of the Maine Attorney General, Defendant reported that 65,010 individuals were affected by the Data Breach. *See* https://apps.web.maine.gov/online/aeviewer/ME/40/a70c625d-eae1-4598-b4d4-29bde6fdb8b7.shtml.

predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. When Defendant learned of the Data Breach;

b. Whether hackers obtained Class members' Private Information via the Data Breach;

c. Whether Defendant's response to the Data Breach was adequate;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

e. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations, industry standards, and/or its own promises and representations;

f. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

g. Whether Defendant owed a duty to Class members to safeguard their Private Information;

h. Whether Defendant breached its duty to Class members to safeguard their Private Information;

i. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class members;

j. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class members;

k. Whether Defendant's conduct was negligent;

l. Whether Defendant's conduct was *per se* negligent;

m. Whether Defendant was unjustly enriched;

n. What damages Plaintiffs and Class members suffered as a result of Defendant's misconduct;

o. Whether Plaintiffs and Class members are entitled to actual and/or statutory damages; and

p. Whether Plaintiffs and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

91. Typicality: All of Plaintiffs' claims are typical of the claims of the Class since Plaintiffs and all members of the Class had their Private Information compromised in the Data Breach. Plaintiffs' claims and damages are also typical of the Class because they resulted from Defendant's uniform wrongful conduct. Likewise, the relief to which Plaintiffs is entitled to is typical of the Class because Defendant has acted, and refused to act, on grounds generally applicable to the Class.

92. Adequacy: Plaintiffs are adequate class representatives because their interests do not materially or irreconcilably conflict with the interests of the Class they seek to represent, they have counsel competent and highly experienced in complex class action litigation, and intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Neither Plaintiffs nor their counsel have any interests that are antagonistic to the interests of other members of the Class.

93. Superiority: Compared to all other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class, a class action is the most superior. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of

the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, Defendant's records and databases.

## VI. CAUSES OF ACTION

### COUNT I
### NEGLIGENCE
**(By Plaintiffs on behalf of the Class, or, in the alternative, the Minnesota Subclass)**

94. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

95. Defendant owes a duty of care to protect the Private Information belonging to Plaintiffs and Class members. Defendant also owes several specific duties including, but not limited to, the duty:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. to protect employees' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. to have procedures in place to detect the loss or unauthorized dissemination of Private Information in its possession;

d. to employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class members;

e. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. to promptly notify Plaintiffs and Class members of the Data Breach, and to precisely disclose the type(s) of information compromised.

96. Defendant also owes this duty because industry standards mandate that Defendant protect confidential Private Information.

97. Defendant also owes this duty because it had a special relationship with Plaintiffs and Class members. Plaintiffs and Class members entrusted their Private Information to Defendant on the understanding that adequate security precautions would be taken to protect this information. Furthermore, only Defendant had the ability to protect its systems and the Private Information stored on them from attack.

98. Defendant also owes a duty to timely disclose any unauthorized access and/or theft of the Private Information belonging to Plaintiffs and the Class. This duty exists to allow Plaintiffs and the Class the opportunity to undertake appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

99. Defendant breached its duties to Plaintiffs and the Class by failing to take reasonable appropriate measures to secure, protect, and/or otherwise safeguard the Private Information belonging to Plaintiffs and Class members.

100. Defendant also breached the duties it owed to Plaintiffs and the Class by failing to timely and accurately disclose to Plaintiffs and Class members that their Private Information had been improperly acquired and/or accessed.

101. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class were damaged. These damages include, and are not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;
- Permanent increased risk of identity theft.

102. Plaintiffs and Class members were foreseeable victims of any inadequate security practices on the part of Defendant and the damages they suffered were the foreseeable result of the aforementioned inadequate security practices.

103. In failing to provide prompt and adequate individual notice of the Data Breach, Defendant also acted with reckless disregard for the rights of Plaintiffs and Class members.

104. Plaintiffs is entitled to damages in an amount to be proven at trial and injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class members.

**COUNT II**
**NEGLIGENCE *PER SE***
**(By Plaintiffs on behalf of the Class, or, in the alternative, the Minnesota Subclass)**

105. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

106. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies, such as Defendant, of failing to use reasonable measures to protect PII and/or PHI. Various FTC publications and orders also form the basis of Defendant's duty. Section 5 of the FTCA imposes a duty on Defendant to provide fair and adequate data security to secure, protect, and/or otherwise safeguard the Private Information of Plaintiffs and Class members.

107. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 requires Defendant to use reasonable measures to protect confidential data.

108. Defendant violated the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to secure, protect, and/or otherwise safeguard Plaintiffs' and Class members' Private Information.

109. Under Minn. Stat. 325E.61 subdivision 1, "any person or business that conducts business in the state, and that owns or licenses data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by

an unauthorized person. The **disclosure must be made in the most expedient time possible and without unreasonable delay** . . . " Minn. Stat. 325E.61, subd. 1.

110. The Data Breach led to the unauthorized access of Plaintiffs' and Class Members' sensitive Private Information. Defendant waited nearly one year to notify Plaintiffs and Class Members that it had discovered the Data Breach, and that the Data Brach impacted their Private Information, including their Social Security numbers. Delaying one year to provide individual notice is an unreasonable delay in violation of Minn. Stat. 325E.61 subdivision 1.

111. Defendant's failure to comply with and the FTCA and the Minnesota data breach notification law constitutes negligence *per se*.

112. Plaintiffs and Class members are within the class of persons that the FTCA and the Minnesota data breach notification law were intended to protect.

113. It was reasonably foreseeable that the failure to protect and secure Plaintiffs' and Class members' Private Information in compliance with applicable laws and industry standards would result in that Information being accessed and stolen by unauthorized actors.

114. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to theft of their personal information, damages from the lost time and effort to mitigate the impact of the Data Breach, and permanently increased risk of identity theft.

115. Plaintiffs and Class members are entitled to damages in an amount to be proven at trial and injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class members.

## COUNT III
## UNJUST ENRICHMENT
**(By Plaintiffs on behalf of the Class, or, in the alternative, the Minnesota Subclass)**

116. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

117. This count is brought in the alternative to Count III.

118. Plaintiffs and the Class have a legal and equitable interest in their Private Information that was collected and maintained by Defendant.

119. Defendant was benefitted by the conferral upon it of Plaintiffs' and Class members' Private Information and by its ability to retain and use that information. Defendant understood that it was in fact so benefitted.

120. Defendant also understood and appreciated that Plaintiffs' and Class members' Private Information was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

121. But for Defendant's willingness and commitment to maintain its privacy and confidentiality, Plaintiffs and Class members would not have provided or authorized their Private Information to be provided to Defendant, and Defendant would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-

security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining customers, gaining the reputational advantages conferred upon it by Plaintiffs and Class members, collecting excessive advertising and sales revenues as described herein, monetary savings resulting from failure to reasonably upgrade and maintain data technology infrastructures, staffing, and expertise raising investment capital as described herein, and realizing excessive profits.

122. As a result of Defendant's wrongful conduct as alleged herein (including, among other things, its deception of Plaintiffs, the Class, and the public relating to the nature and scope of the data breach; its failure to employ adequate data security measures; its continued maintenance and use of the Private Information belonging to Plaintiffs and Class members without having adequate data security measures; and its other conduct facilitating the theft of that Private Information), Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and the Class.

123. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class members' sensitive Private Information, while at the same time failing to maintain that information secure from intrusion.

124. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiffs and the Class in an unfair and unconscionable manner. Defendant's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

125. The benefit conferred upon, received, and enjoyed by Defendant was not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain the benefit.

126. Defendant is therefore liable to Plaintiffs and the Class for restitution in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically the value to Defendant of the PII and private information that was accessed in the Data Breach and the profits Defendant receives from the use and sale of that information.

127. Plaintiffs and Class members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct.

128. Plaintiffs and Class members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

## COUNT IV
## INVASION OF PRIVACY
**(By Plaintiffs on behalf of the Class, or, in the alternative, the Minnesota Subclass)**

129. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

130. Plaintiffs and Class members had a reasonable expectation of privacy in the Private Information that Defendant possessed and/or continues to possess.

131. By failing to keep Plaintiffs' and Class members' Private Information safe, and by misusing and/or disclosing their Private Information to unauthorized parties for unauthorized use, Defendant invaded Plaintiffs' and Class members' privacy by:

a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person; and

b. Publicizing private facts about Plaintiffs and Class members, which is highly offensive to a reasonable person.

132. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' position would consider Defendant's actions highly offensive.

133. Defendant invaded Plaintiffs' and Class members' right to privacy and intruded into Plaintiffs' and Class members' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

134. As a proximate result of such misuse and disclosures, Plaintiffs' and Class members' reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a serious invasion of Plaintiffs' and Class members' protected privacy interests.

135. In failing to protect Plaintiffs' and Class members' Private Information, and in misusing and/or disclosing their Private Information, Defendant has acted with malice and oppression and in conscious disregard of Plaintiffs' and Class members rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing its own economic, corporate, and legal interests above the privacy interests of

its thousands of employees. Plaintiffs, therefore, seeks an award of damages, including punitive damages, on behalf of Plaintiffs and the Class.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all members of the Class, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

A. That the Court certify this action as a class action, proper and maintainable pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3); declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Counsel as Class Counsel;

B. That Plaintiffs be granted the declaratory relief sought herein;

C. That the Court award Plaintiffs and Class members compensatory, consequential, and general damages in an amount to be determined at trial;

D. That the Court award Plaintiffs and Class members statutory damages, and punitive or exemplary damages, to the extent permitted by law;

E. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

F. That the Court award pre- and post-judgment interest at the maximum legal rate;

G. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and

H. That the Court grant all other relief as it deems just and proper.

## DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the putative Class, demand a trial by jury on all issues so triable.

Date: January 31, 2024

Respectfully Submitted,

*/s/ Nathan D. Prosser*

Nathan D. Prosser (MN #0329745)
Lindsey L. Larson (MN #401257)
**HELLMUTH & JOHNSON PLLC**
8050 West 78th Street
Edina, MN 55439
(952) 746-2124
nprosser@hjlawfirm.com
llabellelarson@hjlawfirm.com

Daniel O. Herrera*
Nickolas J. Hagman*
Mohammed A. Rathur*
**CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP**
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com
mrathur@caffertyclobes.com

* *pro hac vice* forthcoming

*Attorneys for Plaintiffs and the Proposed Class*